

AO 106 (Rev. 04/10) Application for a Search Warrant

AUSA: Devon Schulz Telephone: (313) 226-9100
 Special Agent: Todd C. Reineck Telephone: (313) 965-2323

UNITED STATES DISTRICT COURT

for the
 Eastern District of Michigan

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*
 525 E. Trail St. Unit F-1, Jackson, MI 49201
 (more fully described on attachment A)

) Case: 2:19-mc-51731
) Assigned To : Murphy, Stephen J., III
) Assign. Date : 11/27/2019
) SEALED MATTER (MAW)
)
)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See ATTACHMENT A.

located in the Eastern District of Michigan, there is now concealed *(identify the person or describe the property to be seized)*:

See ATTACHMENT B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 2252A(a)(2)	Receipt, and distribution of child pornography
18 U.S.C. 2252(a)(5)(B)	Possession of child pornography

The application is based on these facts:

See attached AFFIDAVIT.

- ☒ Continued on the attached sheet.
☐ Delayed notice _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

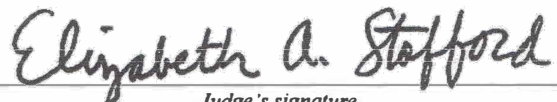
Special Agent, Todd Reineck, FBI

Printed name and title

Sworn to before me and signed in my presence
 and/or by reliable electronic means.

Date: November 27, 2019

City and state: Detroit, Michigan



Judge's signature

Hon. Elizabeth Stafford, U. S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

IN THE MATTER OF THE SEARCH OF)
THE PREMISES LOCATED AT)
) FILED UNDER SEAL
525 E. Trail St. Unit F-1)
Jackson, MI 49201)

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Todd C. Reineck, a Special Agent with the Federal Bureau of
Investigation, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am employed as a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since February 21, 2006. For seven years, I was assigned to the Violent Crimes Squad in Detroit, where I investigated violations involving child sexual exploitation. While assigned to the Violent Crimes Squad, I was a member of the Southeast Michigan Crimes Against Children (SEMCAC) Task Force. In October 2010, I became the task force coordinator for SEMCAC and held that position through June of 2012. As of June 2012, SEMCAC had investigated over 62 cases involving state and federal prostitution, child exploitation, commercial sex trafficking of adults and children, and child pornography. I have been the primary case agent for at least one dozen

investigations of violations involving child pornography and have participated in multiple other investigations of the same. I have received training in investigating child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I am currently assigned to the FBI Flint Resident Agency. In 2017, I started the Northeast Michigan Trafficking and Exploitation Crimes (NEMTEC) Task Force and continued to investigate crimes against children cases. I am currently on a temporary assignment to the FBI Ann Arbor Resident Agency of the Detroit Division of the FBI and continue to investigate crimes involving child sexual exploitation.

2. I am conducting an investigation related to violations of the following statutes: receipt and distribution of child pornography, in violation of 18 U.S.C. § 2252A(a)(2), and possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). Based on the evidence discovered during my investigation, I have probable cause to believe that evidence related to the above offenses is located within the premises described as 525 E. Trail St. Unit F-1, Jackson, MI 49201 (Subject Premises).

3. Consequently, I am submitting this affidavit in support of a search warrant authorizing a search of 525 E. Trail St. Unit F-1, Jackson, MI 49201. I am requesting authority to search the entire Subject Premises, including the residential

dwelling, any detached storage buildings or garages, and any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of a crime.

4. I am aware that many computers and electronic storage devices today—such as laptop computers, tablets, telephones, external drives, and thumb drives—are portable. I also know from my training and experience that these devices are often stored in vehicles to prevent other users in the home from discovering the existence of the child pornography collection. Therefore, this application seeks permission to search vehicles located at or near the premises that fall under the dominion and control of the person or persons associated with said premises. The search of these vehicles is to include all internal and external compartments and all containers that may be capable of storing computer media or other repositories associated with the storage of child pornographic materials or their instrumentalities contained within the vehicles.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to

establish probable cause to believe that evidence and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2), receipt and distribution of child pornography, and 18 U.S.C. § 2252A(a)(5)(B), possession of child pornography, are presently located at 525 E. Trail St. Unit F-1, Jackson, MI 49201 (Subject Premises).

PROBABLE CAUSE

6. On or about September 25, 2019, an FBI employee acting in an undercover capacity (online undercover employee or OCE) conducted an investigation into the sharing of child pornography files on LIVEME. LIVEME is a free mobile application that can be downloaded on Android or iOS devices that permits users to stream live video of themselves to an anonymous audience of fellow LIVEME users. The users in the audience can post comments and interact with the user/users streaming the video. LIVEME creates a unique identifier, typically a string of numbers, for each individual user. Each user also has the ability to create a screen name, which can be changed at any time.

7. LIVEME allows users to create “groups,” where like-minded individuals can chat with and text other users and post videos and images to the group’s LIVEME page. During the course of their investigation, the OCE identified several groups that appeared, based on their names, to be involved in the sharing of child pornography. The OCE could see who the members or “fans” of the various LIVEME groups were, but could not see groups’ pages without

becoming a member. To try and become a member of these groups, the OCE sent requests to the owners of these groups stating that the OCE had child pornography to share or trade. The OCE was granted access to multiple groups, including “wicked pervs,” “Young Girl Lover,” “Lil Lola,” and “You Know.” The OCE discovered that the members of these groups were focused on distributing images of child pornography within the LIVEME groups.

8. Specifically, in the group “wicked pervs,” the OCE observed that hundreds of images and videos of child pornography and links to child pornography were distributed by the members of the group. Members of the group posted these images and links to the group’s page, where the posts were viewable and accessible by other members of the group. The OCE told me that the images and videos posted in “wicked pervs” are described as prepubescent children, including infants and toddlers, who are being sexually assaulted by adults and other children.

9. The OCE learned that an individual with the LIVEME profile identifier 158814930, using screenname Stroke4You13, was a member or “fan” of multiple groups that appeared to be focused on the sharing of child pornography, including groups that the OCE accessed and observed to be engaged in the sharing of child pornography. For example, Stroke4You13 was a member of “Young Girl Lover,” “You Know,” and “wicked pervs,” described above. The OCE was able to

view Stroke4You13's profile and could see that Stroke4You13 was a member or "fan" of these groups.

10. The OCE observed that on or about September 25, 2019, Stroke4You13 posted a video to the group "wicked pervs" depicting a nude prepubescent girl being vaginally raped with a large object by a nude adult male wearing a clown mask. I believe the video was posted on or about September 25, 2019, because the timestamp on Stroke4You13's account stated the video was posted "Yesterday 11:07 AM," and the video was screen-recorded by the OCE on September 26, 2019. On or about October 29, 2019, I reviewed this video and determined that it meets the federal definition of child pornography.

11. On or about September 30, 2019, the OCE sent a subpoena to LIVEME requesting user data for Stroke4You13. On or about October 3, 2019, and again on October 9, 2019, the OCE received records from LIVEME, which showed that Stroke4You13's most recently used IP address 23.122.221.38 (Suspect IP) to log into LIVEME on October 9, 2019. This is not the IP address that was used on the date and time that Stroke4You13 posted the above-described video of child pornography to the group "wicked pervs." However, the Suspect IP was listed as Stroke4You13's last registration IP address on August 26, 2019, and it is Stroke4You13's most frequently used IP address. LIVEME provided approximately 588 login events, and approximately 340 of those were from the

Suspect IP.

12. The information provided by LIVEME also identified Stroke4You13's device as an "LG-Q710AL." This is the device that was used on the date and time that Stroke4You13 posted the above-described video of child pornography to the "wicked pervs" group. I searched for this device on the internet and determined it to be an LG Stylo 4 smart phone.

13. On or about October 3, 2019, the OCE used an open source website and determined that AT&T is the internet service provider (ISP) for the Suspect IP. On the same day, OCE sent a subpoena to AT&T requesting subscriber information for the Suspect IP.

14. On or about October 5, 2019, the OCE received the subpoena return from AT&T and learned that the Suspect IP is assigned to Steven Skeens, with service at 525 E. Trail St., Unit F-1, Jackson, MI 49201 (Subject Premises), using telephone number 517-395-0523, and email address twizidclown311@gmail.com. The account was still active as of October 5, 2019. The investigation was turned over to the Detroit Division, Ann Arbor Resident Agency.

15. According to the Jackson County Tax and Property records, the Subject Premises is owned by a third party who lives in Nashville, Tennessee. However, I queried Steven Skeens in Thompson Reuter's CLEAR database and learned that the Subject Premises is associated with Skeens. I also learned, from a

check of Michigan Secretary of State records, that the Subject Premises is listed on Skeens's driver's license.

16. On October 24, 2019, I conducted physical surveillance at the Subject Premises. While conducting surveillance, I observed two vehicles in the driveway. The first was a blue Ford F150 and the second was a Buick Riviera. I ran the license plates through the Law Enforcement Information Network (LEIN). The Buick Riviera was registered to R.D., who I later learned resides in the residence above the Subject Premises. The blue Ford F150 was registered to a third party. I know, based on a review of Michigan Secretary of State records, that a 2005 Ford Taurus, bearing Michigan license plate ECQ7796, is registered to Skeens at the Subject Premises.

17. Also while conducting surveillance, I determined that the Wi-Fi networks available and accessible at and around the Subject Premises were password-protected. I determined this by searching for, and attempting to connect to, nearby Wi-Fi networks on my phone.

18. On October 25, 2019, I learned, from agents with the Postal Inspection Service, that Skeens currently receives mail at the Subject Premises. Specifically, Skeens receives mail to the lower unit, F-1. The downstairs unit, F-1, is accessed by the front door facing Trail Street and the door located on the left side near the bottom of the exterior stairwell. I also learned from the agents with

the Postal Inspection Service that the Subject Premises is a single-family dwelling that had been converted into upstairs and downstairs living units.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

19. Based upon my knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals involved in the receipt and collection of child pornography, including the following:

- a. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- b. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification.

Skeens's distribution of the above-described child pornography video in the LIVE ME group "wicked pervs" demonstrates that he has a

sexual interest in children and is likely a collector of child pornography. Moreover, based on the evidence uncovered during this investigation, Skeens possessed and distributed at least one image/video that meets the federal definition of pornography.

- c. Individuals who have an interest in child pornography almost always possess and maintain their “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location;
- d. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment. These collections are often maintained for several years and are kept close by, usually at the collector’s residence, to enable the collector to view the collection, which is valued highly;
- e. Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit

material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. The evidence uncovered in this investigation has shown that Skeens corresponds with others who share an interest in child pornography because he is a member of the LIVEME group “wicked pervs.” The OCE became a member of “wicked pervs” and learned that members of this group were posting and distributing child pornography.

- f. Collectors of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Moreover, the nature of the materials, their attraction to the materials, and the risk involved with producing, receiving, downloading, and possessing such materials, motivates collectors to keep their child pornography collection within their possession and control wherever they go. Because collectors of child pornography place an extremely high value on their collection, they will take their collection with them if they move from one location to another.

20. Based on his membership in the group “wicked pervs,” and other LIVEME groups that appear to be engaged in the sharing of child pornography, and based on the child pornography video he posted to the group “wicked pervs,” Skeens, who is believed to be using the username Stroke4You13, displays characteristics common to individuals who possess, collect, receive, and/or produce child pornography. Therefore, there is probable cause to believe that child pornography and evidence of his involvement in its receipt and production will be located on electronic devices at the Subject Premises.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

21. I know, based on training and experience, that computers and cellular telephones are a common tool to create, store and/or share photographs, files, documents. Because modern cell phones/smart phones contain many of the same features as a traditional computer, as used in this affidavit, the terms “computer,” “hard drive,” and “computer storage device” is used interchangeably with “cell phone,” “smart phone,” and “cell phone storage device.”

22. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage and social networking.

23. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the

images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

24. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

25. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

26. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used,

however, evidence of child pornography can be found on the user's computer in most cases.

27. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

28. Based on my training and experience, I know that images taken with a camera, built into a cellular phone, or images stored on a cellular phone, may be transferred and stored onto a computer. The transfer may occur when the phone is connected, through a cable, directly to the computer. The transfer may also occur through the Internet, with e-mail, or other software if the phone can access the Internet through a cellular network or a Wi-Fi router.

29. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history

files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or “slack space” – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten.

30. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an

electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

31. It is difficult to know, prior to the search, which exact method of extracting the evidence will be needed and used and which expert possesses sufficient specialized skills to best obtain the evidence and subsequently analyze it. No matter which method is used, the data analysis protocols that will be utilized are exacting scientific procedures, designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Upon approval and execution of the search warrant, in appropriate circumstances, a forensic image (also known as a bit-stream image), which is an exact physical copy of the seized electronic evidence, will be created so that their contents could be examined at a field office or computer laboratory and/or other locations following completion of the on-site search.

32. The search of computers, hard drivers, and other seized electronic media will include a complete search of the entire piece of seized electronic evidence. A computer forensic examiner cannot rely on the name of a file to exclude or confirm the existence of child pornography within that file. Individuals will

intentionally mislabel directory structures, folder names, and filenames to hide the presence of child pornography. In other cases, an individual may not attempt to hide the child pornography but utilize a unique naming convention or organizational methodology which may inadvertently hide the presence of child pornography. In order to perform a comprehensive forensic examination, a computer forensic examiner must conduct an all-inclusive examination of every bit (or binary digit) on the particular electronic storage device.

33. Moreover, hard drives and other pieces of electronic media have unallocated space which might contain deleted files, records, relevant e-mails, other communications, and search terms related to the possession, receipt, and distribution of child pornography. Thus, without looking at the entirety of the electronic media for evidence related to child pornography, the investigator may not find evidence relevant to the criminal investigation.

34. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of millions of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site; and
- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal

activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

35. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

36. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

**SEARCH METHODOLOGY TO BE EMPLOYED
FOR ELECTRONIC MEDIA**

33. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. On-site triage of computer system(s) to determine what, if any, peripheral devices and/or digital storage units have been connected

to such computer system(s), as well as a preliminary scan of image files contained on such system(s) and digital storage device(s) to help identify any other relevant evidence and/or potential victim(s);

- b. Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- c. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- d. Surveying various file directories and the individual files they contain;
- e. Opening files in order to determine their contents;
- f. Scanning storage areas;

g. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or

g. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

CONCLUSION

37. Based on the facts of this investigation, detailed above, coupled with my training and experience as a FBI Special Agent, there is probable cause to believe that Steven Skeens is a collector of child pornography and is engaging in violations of 18 U.S.C. § 2252A(a)(2), receipt and distribution of child pornography, and 18 U.S.C. § 2252A(a)(5)(B), possession of child pornography. Therefore, there is probable cause to believe that evidence and instrumentalities of those criminal offenses, more fully described in Attachment B, are located in Skeens's residence at 525 E. Trail St. Unit F-1, Jackson, MI 49201, more fully described in Attachment A. This is because of the following:

- LIVEME user Stroke4You13 is a member of the group "wicked pervs," in which members share child pornography;
- Stroke4You13 posted a video of child pornography to that group;
- Stroke4You13's most recent registration IP address and most

frequently used IP address is the Suspect IP;

- The Suspect IP is registered to Skeens at the Subject Premises;
- Skeens currently receives mail to the Subject Premises and the Subject Premises is listed on his Michigan driver's license.

REQUEST FOR SEALING

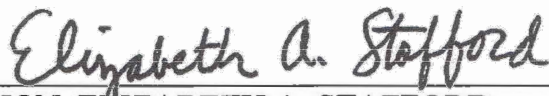
38. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,



Todd C. Reineck
Special Agent, Federal Bureau of
Investigation

Sworn to before me and signed in my
presence and/or by reliable electronic means.



HON. ELIZABETH A. STAFFORD
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF MICHIGAN

November 27, 2019

ATTACHMENT A

DESCRIPTION OF THE PREMISES TO BE SEARCHED

The Subject Premises is located at 525 E. Trail St. Unit F-1, Jackson, MI 49201. The residence is described as a two story house with blue aluminum siding. The numbers “525” can be seen to the left of the front door above the mailbox. The apartment to be searched—Unit F-1—is on the main floor of the house.



ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

1. Any and all cellular phones, including an LG Stylo 4 smart phone.
2. Any computer(s), cellular phones (including an LG Stylo 4 smart phone), removable digital media, computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
3. Evidence of who used, owned, or controlled the computer(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, accounts of Internet Service Providers.
4. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence, rental or lease agreements, mortgage documents, rental or lease payments and credit card information, including, but not limited to, bills and payment records.

5. Any and all notes, documents, records, computer files or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), including communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography or membership in online groups, clubs, or services that provide or make accessible child pornography to members.

6. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

7. Any and all cameras, film, videotapes or other photographic equipment that may be used to commit or facilitate commission of violations of 18 U.S.C. §§ 2251, 2252 and 2252A.

8. Any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual

depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

9. Any and all visual depictions of minors.

Hon. Elizabeth Stafford, U. S. Magistrate Judge
Printed name and title

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title